Additional Management Actions Are Needed to Enhance Data Security When Processing User Fee Payment Information

May 2001

Reference Number: 2001-10-091

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

May 24, 2001

MEMORANDUM FOR COMMISSIONER, TAX EXEMPT AND GOVERNMENT ENTITIES DIVISION

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Additional Management Actions Are Needed to Enhance Data Security When Processing User Fee Payment Information

This report presents the results of our review of administrative controls for the security of data maintained on Tax Exempt and Government Entities (TE/GE) Division's automated systems used to process user fee payment information. In summary, we found that additional actions are needed to better manage the data security risks when processing user fee payment information on TE/GE Division automated systems.

Our recommendations will increase assurances that TE/GE management has taken appropriate steps to ensure that user fee payment data are properly safeguarded. TE/GE Division management agreed with all but one of the recommendations presented in the report. The TE/GE Division elected to not develop specific disaster and business resumption plans for the Letter Information Network User System (LINUS). Rather, the TE/GE Division will use the Business Resumption Plan developed for the Ohio area office. We do not concur with the TE/GE Division's decision to not develop specific disaster and business resumption plans for the LINUS. The risks associated with using the Business Resumption Plan are increased because the Business Resumption Plan for the Ohio area office does not specifically identify or refer to the LINUS. Management's comments have been incorporated into the report where appropriate, and the full text of their comments is included as an appendix.

Copies of this report are being sent to the Internal Revenue Service managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you

have questions, or Maurice S. Moody, Associate Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs), at (202) 622-8500.

Table of Contents

Executive Summary

The Tax Exempt and Government Entities (TE/GE) Division has initiated actions to develop a new automated system to improve management and accounting controls for processing user fee payments. During Fiscal Year (FY) 2001, the TE/GE Division plans to begin redesigning the Employee Plans and Exempt Organizations (EP/EO) Determination System (EDS)[1] to allow the Division to fully meet its objective of providing timely, accurate, and consistent service to its customers.

The objective of this audit was to determine whether the TE/GE Division's automated systems used to process user fee payment information provide reasonable assurance that data are properly protected. We evaluated various administrative controls for the security of data maintained on the Letter Information Network User System (LINUS)[2] and the Headquarters Employee Plans/Exempt Organizations Inventory System (HQ EP/EO system).[3]

Results

Even though TE/GE Division management has taken some steps to protect customer user fee payment information, additional actions are needed to better manage the data security risks on existing systems. Timely addressing these risks is critical to ensuring that current and future user fee payment information is secure. To effectively manage the risks associated with processing user fee payment information, TE/GE Division management should:

- Establish oversight responsibility for the security of data maintained on the current automated systems.
- Strengthen data security controls for the LINUS.

[1] The EDS is the TE/GE Division's inventory system that controls the EP/EO customer applications from receipt to issuance of the determination letter.
[2] The LINUS is used to control user fee payment information provided by customers who submit EP/EO applications.
[3] The user fee payment information is maintained on a mid-range computer system maintained at the Martinsburg Computing Center.

Additional Actions Are Needed to Better Manage the Data Security Risks When Processing User Fee Payment Information

The current management structure does not provide the Commissioner, TE/GE Division, with reasonable assurance that adequate data security is provided when processing user fee payment information on current automated systems. The LINUS and HQ EP/EO automated systems used to process user fee payment information are not properly certified or accredited as secure systems. Without proper certification and accreditation, TE/GE Division management would not be in a position to protect sensitive customer data. These conditions exist because TE/GE Division management has not established clear roles and responsibilities for system security certification.

Computer Security Controls Established for the Letter Information Network User System Could Be Strengthened

The TE/GE Division developed the LINUS to facilitate the processing of user fee payments that are forwarded to the Ohio area office. Although the LINUS was never intended to meet all of the TE/GE Division's business needs for user fee processing systems, we believe additional actions should be taken to enhance the security of sensitive customer data currently maintained on the system. Specifically, we found that: the LINUS user identification controls needed to be strengthened; a process had not been implemented to ensure the LINUS meets established security-monitoring requirements; the LINUS was not listed on the Sensitive Systems Inventory Listing; and, the LINUS Disaster Recovery and Business Resumption Plans had not been completed. These actions were not taken because security over data maintained on the LINUS was never assigned to a responsible management official. Assigning responsibility for these actions would enhance the TE/GE Division's efforts to safeguard information against unauthorized accesses, disclosure, damage, modification, and theft.

Summary of Recommendations

Even though TE/GE Division management has taken some steps to protect customer user fee payment information, additional actions are needed to better manage the data security risks. Specifically, we determined that additional management emphasis is needed to properly certify and accredit user fee systems and to establish overall responsibility for managing TE/GE Division user fee systems. Also, the TE/GE Division should appoint a functional security coordinator for the LINUS and develop a process for identifying and reporting TE/GE Division automated systems with sensitive information to the Certification Program Office. Additionally, a process should be developed to ensure that Disaster Recovery and Business Resumption Plans are established for the LINUS.

Management's Response: IRS management agreed with all but one recommendation cited in the report and is taking appropriate corrective actions. The Commissioner,

TE/GE Division, has emphasized the importance of ensuring that automated systems are properly certified and has established controls to ensure that the TE/GE Division does not deploy new systems without the appropriate security certifications. In addition, the TE/GE Division will establish a service-level agreement with the Information Systems (IS) organization to ensure that all system development initiatives adhere to the IRS' Enterprise Life Cycle process for security certifications and data safeguards.

The Commissioner, TE/GE Division, has directed that audit trail information be produced and reviewed for the LINUS system and the HQ EP/EO replacement system, and the Director, EO Rulings and Agreements, will appoint a functional security coordinator for the LINUS. The TE/GE Division will also develop a systems inventory matrix that will identify any system with sensitive information not reported to the IS organization and ensure that these systems are properly registered with the IS Certification Program Office.

The TE/GE Division elected to not develop specific disaster and business resumption plans for LINUS because this system has a limited life. Rather, the TE/GE Division will use the IS Business Resumption Plan developed for the Ohio area office until a LINUS replacement system is developed.

Office of Audit Comment: We do not concur with the TE/GE Division's decision to not develop specific disaster and business resumption plans for the LINUS. The risks associated with using the IS Business Resumption Plan are increased because the IS Business Resumption Plan for the Ohio area office does not specifically identify or refer to the LINUS. The time period to develop the LINUS replacement system may exceed the scheduled calendar year 2002 implementation date, resulting in additional risks that user fee payment information may be lost.

Management's comments are included in the body of the report where appropriate, and the complete text of their response is included as Appendix IV.

Objective and Scope

We evaluated various administrative controls for the security of data maintained on the TE/GE Division's automated systems used to process user fees.

The objective of this audit was to determine whether the Tax Exempt/Government Entities (TE/GE) Division's automated systems used to process user fee payment information provide reasonable assurance that data are properly protected. We evaluated various administrative controls for the security of data maintained on the Letter Information Network User System (LINUS)[1] and the Headquarters Employee Plans/Exempt Organizations Inventory System (HQ EP/EO System).[2] Specifically, we:

- Evaluated TE/GE Division's management oversight of automated user fee processing systems.
- Evaluated the process used to coordinate security requirements with other Internal Revenue Service (IRS) organizations.
- Assessed security controls established for the automated user fee processing systems.

To accomplish our objective, we evaluated data security policies and procedures for processing user fee payments and interviewed TE/GE Division and Information Systems (IS) organization (Strategic Planning and Client Services) management officials and employees.

This audit was performed at the National Headquarters, the TE/GE Division Headquarters office, the Cincinnati Submission and Processing Center (CSPC), and the Ohio field office between March and November 2000, and it was conducted in accordance with *Government Auditing Standards.*

[1] The LINUS is used to control user fee payment information provided by customers who submit Employee Plans and Exempt Organizations (EP/EO) applications.

[2] The user fee payment information is maintained on a mid-range computer system maintained at the Martinsburg Computing Center.

Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

Background

Section 105-11 of the Revenue Act of 1987[3] provides that the Secretary of the Treasury or his delegate shall establish the payment of user fees for requests to the IRS for rulings, opinions, determinations, and similar actions. User fee amounts, which are specified by statute, range from $80 to $10,000. EP/EO determination letter requests are forwarded to the CSPC where user fee payments are processed and deposited with a Federal Reserve Bank. The user fee and application information is input into the LINUS and acknowledgement letters are sent to the applicant. Other user fees submitted for revenue rulings and opinions are received at the TE/GE Division Headquarters office. Information associated with these user fees is input into the HQ EP/EO system and acknowledgement letters are sent to the applicants. During Fiscal Year (FY) 1999, the TE/GE Division processed a total of $34.5 million in user fee payments.

Office of Management and Budget (OMB) and Department of the Treasury guidelines require that all information systems that process sensitive but unclassified information be certified and accredited and meet specified security requirements. The accreditation should be performed by TE/GE Division senior management to ensure that customer data are adequately safeguarded on their automated systems.

[3] Pub. L. No. 100-203, 101 Stat. 1330-382, 1330-446 (1987).

Results

The TE/GE Division is taking actions to develop a new automated system to improve management and accounting controls for processing user fee payments.

The TE/GE Division is taking actions to develop a new automated system to improve management and accounting controls for processing user fee payments. During FY 2001, the TE/GE Division plans to begin redesigning the EP/EO Determination System (EDS)[4] to allow the TE/GE Division to fully meet its objective of providing timely, accurate, and consistent service to its customers. One of the major business initiatives to be delivered by the redesigned system is the enhancement of processing, accounting, and researching of user fee payment information.

Additional actions are needed to establish overall responsibility that will ensure end-to-end accountability for managing the security of user fee payment information systems.

Even though TE/GE Division management has taken some steps to protect customer user fee payment information, additional actions are needed to better manage the data security risks on existing systems. Management actions are also needed to establish overall responsibility that will ensure end-to-end accountability for managing the security of the user fee payment information systems. The TE/GE Division has not incorporated the concept of a senior-level person with end-to-end accountability for managing these systems.

Additional Actions Are Needed to Better Manage the Data Security Risks When Processing User Fee Payment Information

The Commissioner, TE/GE Division, is the principal accrediting authority for the TE/GE Division's business systems that contain sensitive but unclassified information. IRS procedures require the Commissioner, TE/GE Division, to certify that security measures are reasonable, adequate, and effectively implemented on

[4] The EDS is the TE/GE Division's inventory system that controls the EP/EO customer applications from receipt to issuance of the determination letter.

TE/GE Division automated systems that process customer data.

The current management structure does not provide the Commissioner, TE/GE Division, with reasonable assurance that adequate data security is provided when processing user fee payment information.

The current management structure does not provide the Commissioner, TE/GE Division, with reasonable assurance that security measures are reasonable, adequate, and effectively implemented. This condition exists because TE/GE Division management has not established clear roles and responsibilities for system security certification. We believe TE/GE Division senior management needs to take a more active role to ensure that the automated systems provide adequate security. Without proper certification and accreditation, TE/GE Division management would not be in a position to protect sensitive customer data.

The HQ EP/EO system is currently processing sensitive customer data without the proper certification

The HQ EP/EO system is listed as a system with sensitive but unclassified information on the IRS' Sensitive Systems Inventory Listing (SSIL). However, the certification performed by the IS organization for the HQ EP/EO system expired in 1998 and, as a result, the HQ EP/EO system is currently processing sensitive customer data without being properly certified or accredited. Required documentation that has not been completed for the certification process includes the Continuity of Operations Plan and the Trusted Facility Manual Access Control Listing. Additionally, the HQ EP/EO system does not meet the security monitoring requirements for systems that process sensitive customer data. For example, the system does not generate audit trail information that would identify inappropriate system accesses. Without the proper certification of the automated systems, the Commissioner, TE/GE Division, may be unable to provide the necessary assurance that user fee payment information is secure.

Even though the IS organization is the system owner, the TE/GE Division should provide the required assurances that the automated systems it uses to process taxpayer payment data are secure.

The TE/GE Rulings and Agreements organization uses the HQ EP/EO system to process user fee payments in its Headquarters office. The IS organization is its owner and, as a result, is responsible for conducting the necessary steps that will result in the certification that the system will process data in a secure environment. Even though the IS organization is the system owner, IRS security procedures require the TE/GE Division to provide the required assurances that the automated systems it uses to process taxpayer user fee payment data are secure.

Additional management oversight is needed to ensure that the TE/GE Division receives appropriate IS support. For example, there is no senior TE/GE manager with overall responsibility for the HQ EP/EO system. The TE/GE Division must rely on the IS organization for conducting the certification processes even though the TE/GE Division is the process owner.

The LINUS does not have a security certification or accreditation filed with the IRS Certification Program Office

The LINUS contains sensitive taxpayer information but it does not have a security certification or accreditation with the IRS Certification Program Office. The OMB Circular A-130, *Management of Federal Information Resources*, and the Department of the Treasury Security Manual require that all information systems that process sensitive data be certified and accredited prior to being placed in operation. The security certification process determines the extent to which a system meets a specific set of security requirements. Accreditation is the issuance of an official statement by the responsible official that he/she authorizes the use of the system and accepts its level of risk. IRS functional executives are responsible for the accreditation of IRS information systems. Without an established process to certify the security of data processed on the LINUS, TE/GE Division management cannot provide the required assurance that user fee payment information is adequately safeguarded.

We did not identify a senior-level manager with overall responsibility for the LINUS.

We did not identify a senior-level manager with overall responsibility for the LINUS. The Director of the TE/GE Business Systems unit stated that senior management had not delegated the responsibilities for the LINUS because the system is still in the start-up phase. The local TE/GE Division Office Automation group manager in Cincinnati is currently performing the day-to-day management of the LINUS.

The service-level agreement with the IS support organization does not ensure that sensitive customer data will be protected

The TE/GE Division's existing practices do not ensure that sufficient support for data security will be provided by the IS organization since service-level agreements have not been developed for the security services to be provided by the IS organization. The existing service-level agreement with the IS organization does not include provisions for performing systems certification. We were advised by TE/GE Division management that any future agreements with the IS organization will specify that the IS organization "operate" the entire automated system and, therefore, the agreements will not specifically address computer security requirements.

The TE/GE Division created the Business Systems unit to support its information systems needs. This group is responsible for information systems strategy, planning, and coordinating and for monitoring the support provided by the IS organization. One of its main objectives is to oversee the TE/GE Division's contractual relationship with the IS organization to ensure that adequate services are provided. The Director's role and responsibility for the Business Systems unit includes ensuring that service-level agreements between the TE/GE Division and IS organization cover all aspects of IS technology related to TE/GE Division business systems.

Organizational boundaries should not prevent the TE/GE Division from monitoring the adequacy of the computer security support that may be provided by the IS organization.

Although the service-level agreement did not specifically include security services, sound business practices dictate that organizational boundaries should not prevent the TE/GE Division from monitoring the adequacy of the computer security support that may be provided by the IS organization. Security requirements should be incorporated into an effective service-level agreement for automated systems under the ownership of the IS organization. In addition, TE/GE management should monitor the adequacy of the support they receive from the IS organization to ensure these requirements are being met. A failure to establish controls to oversee the security of automated systems used by the TE/GE Division could adversely affect the Division's efforts to protect sensitive customer data. The TE/GE Division could also be at risk of accrediting a system with inadequate security because the Commissioner, TE/GE Division, becomes the principal accrediting authority and accepts responsibility for the security of the system when the certification is completed.

Management has not established clear guidance regarding the roles and responsibilities for certifying system security. The Director, TE/GE Business Systems unit, advised us that computer security oversight of the HQ EP/EO system was an IS organization responsibility. He stated that the TE/GE Division will rely on local IS support when security reviews are performed.

Establishing a senior-level manager with end-to-end accountability for managing the HQ EP/EO system and the LINUS would enhance the process used to provide the Commissioner, TE/GE Division, with the assurance that these automated systems have sufficient security controls in place that provide an acceptable level of risk.

Recommendations

The Commissioner, TE/GE Division, should:

1. Emphasize the need to implement processes that will ensure that the TE/GE Division systems are properly certified and accredited.

2. Establish a senior-level manager with overall responsibility for managing the security of data for the TE/GE Division's automated systems.

3. Enhance the service-level agreement with the IS organization to ensure that the TE/GE Division's automated systems are timely certified that data will be properly safeguarded.

Management's Response: The Commissioner, TE/GE Division, emphasized to appropriate managers the importance of ensuring that TE/GE systems are properly certified. The TE/GE Division Business Systems Planning organization was established to ensure that all TE/GE Division automated systems are developed using the IRS' Enterprise Life Cycle (ELC) process to ensure that new systems are not deployed without the appropriate security certification.

The Director, Business Systems Planning, and the Division Information Officer will develop a systems inventory matrix to capture and document important information for each of the business systems on which the TE/GE Division relies. The matrix will include: system management points of contact, platform and user characteristics, data types, and the status of security certifications and disaster recovery and business resumption plans. This matrix will give the Commissioner, TE/GE Division, a basis for monitoring changes and prioritizing follow-up or remedial actions.

The TE/GE Division is planning a service-level agreement with the IS organization. The TE/GE Division requires that all system development initiatives adhere to the IRS' ELC process. This requirement will help ensure that new systems are not deployed without appropriate security certifications and data safeguards.

Computer Security Controls Established for the Letter Information Network User System Could Be Strengthened

TE/GE Division management developed the LINUS to facilitate the processing of user fee payments forwarded to the Ohio area office. Although the LINUS was never intended to meet all of the TE/GE Division's business needs for user fee processing systems, we believe additional actions should be taken to enhance the security of sensitive customer data currently maintained on the LINUS.

Additional actions should be taken to enhance the security of sensitive customer data currently maintained on the LINUS.

Specifically, we found that additional actions could be taken to:

- Strengthen user identification controls.
- Implement a process to ensure that the LINUS meets established security-monitoring requirements.
- Ensure the completion of a Disaster Recovery and Business Resumption Plan.

These actions were not taken because security over the data maintained on the LINUS was never assigned to a responsible management official. Assigning responsibility for these actions would enhance the TE/GE Division's efforts to safeguard information against unauthorized access, disclosure, damage, modification, and theft.

The LINUS user identification controls need to be strengthened

The LINUS is at risk that an employee could circumvent the system's audit trail

Readily available employee identification numbers (EIN) are currently used as passwords to access the LINUS. They identify the employee who is entering information into the LINUS. EINs are not secure, protected passwords because they are widely known by other employees. As a result, there is a risk that an employee could successfully circumvent the system's audit trail by using another employee's EIN. The LINUS Systems Administrator stated that he used employee numbers as LINUS passwords because they

had been used for accessing the prior system that the LINUS replaced.

Secure user identification passwords are required to protect the integrity of the audit trail. They are also needed to authenticate the user's identity and identify all system accesses initiated by that individual. If the audit trail can be successfully circumvented, then all audited actions may become unreliable.

The LINUS was never designed to generate and/or accept secure user identification passwords. The Statement of Work used to develop the LINUS did not discuss the need to use secure password information. This omission may have contributed to the use of EINs as user identification passwords.

Processes have not been established to ensure the LINUS meets security monitoring requirements

Each executive, who is head of the office where an application or system with sensitive but unclassified information resides, is required to select functional security coordinators to administer the security requirements for his/her information systems. The functional security coordinators are required to perform:

- Periodic functional security reviews of each information system.
- Selective reviews of employee actions using audit trail information generated by the automated system.

Our review identified the following security monitoring control weaknesses for the LINUS:

- The system did not have a designated functional security coordinator.
- No provisions were made to generate the audit trail reports for review of system accesses.
- Functional security reviews were not being performed.

There was no designated security administrator for the LINUS.

IRS procedures require the functional security coordinator to review audit trail information. The LINUS Systems Administrator stated that there was no designated security administrator for the system because he was never instructed to designate a security administrator and, as a result, no one was assigned responsibility for producing and reviewing audit trail reports. Unauthorized system accesses may go undetected when audit trail information is not reviewed.

The LINUS is not listed on the SSIL

The LINUS contains sensitive customer data, but it is not listed on the SSIL.

The LINUS contains sensitive customer data, but it is not listed as a system with sensitive information on the SSIL. IRS procedures require an inventory of all systems that process sensitive customer information. The Certification Program Office, under the direction of the Office of Security and Privacy Oversight, maintains and updates the SSIL. Field organizations are responsible for reporting local sensitive systems to their appropriate Chief Officer's Security Plan Coordinator for addition to the SSIL. We did not identify any controls to ensure that TE/GE Division-owned systems are reported to the Office of Security and Privacy Oversight for addition on the SSIL. Also, there was a lack of awareness of the certification and SSIL requirements. Neither the Ohio field office management team nor the LINUS Systems Administrator was aware of the SSIL requirement.

Additionally, there was no TE/GE Division management official designated with the responsibility for reporting systems with sensitive but unclassified information to the Certification Program Office. Not listing automated systems on the SSIL could result in these systems not being timely certified that security measures are reasonable, adequate and effectively implemented.

The LINUS Disaster Recovery and Business Resumption Plans have not been completed

The Statement of Work document used to develop the LINUS did not identify any requirement to develop a disaster recovery plan. The ELC process requires the

development of a disaster recovery plan and a system contingency plan to ensure that proper back-up and recovery procedures are in place in the event of a system failure.

Neither a Disaster Recovery Plan nor a Business Resumption Plan was developed for the LINUS.

The Ohio field office management team advised us that neither a Disaster Recovery Plan nor a Business Resumption Plan was specifically developed for the LINUS because the IS Business Resumption Plan developed for the Ohio area office could be used in lieu of any specific plans for LINUS. However, the local Business Resumption Plan did not identify any specific reference to the LINUS.

Recommendations

The Commissioner, TE/GE Division, should:

4. Ensure that automated systems require unique and secure password information and the ability to monitor employee accesses.
5. Emphasize the need to generate audit trail reports for review of system accesses on all systems used to process user fee payment information.
6. Appoint a functional security coordinator for the LINUS who will conduct periodic functional security reviews using system-generated audit trail information.
7. Develop a process for identifying and reporting the TE/GE Division's automated systems with sensitive information to the Certification Program Office.
8. Develop a process to ensure that the Disaster Recovery and Business Resumption Plans are developed for the LINUS.

Management's Response: The TE/GE Division will require that system development initiatives adhere to the ELC process to ensure that security certifications are appropriate for the data processed by the automated system before the system is deployed. The TE/GE Division has requested that the IS security organization

provide a vulnerability assessment of the LINUS. The assessment will identify any necessary cost effective interim solutions for a system with a limited life. The TE/GE Division will request that IS initiate the necessary actions to respond to the needs identified.

The TE/GE Division plans to migrate the HQ EP/EO system from its current hardware platform to a new platform. The new hardware will have sufficient capacity to generate audit trail reports and the Director, EO Rulings and Agreements, will require the HQ EP/EO data base administrator to generate audit trail reports for review by the functional security coordinator. The Director, EO Rulings and Agreements, will require the LINUS data base administrator to produce audit trail reports and appoint a LINUS functional security coordinator to review the reports.

The Director, Business Systems Planning, and the Division Information Officer will develop a systems inventory matrix to capture and document important information for TE/GE Division automated systems. The matrix will identify, and the TE/GE Division will report, any system with sensitive information not reported to the IS Certification Program Office. The TE/GE Division will require developers of new systems to comply with the ELC process to ensure that appropriate security processes are developed before the new systems are deployed.

The TE/GE Division is designing a new system that will replace the LINUS. The design of the new user fee processing system will follow the ELC process. This process requires that the TE/GE Division develop a disaster recovery and business resumption plan for the new system. Until the replacement user fee processing system is operational, the TE/GE Division will use the disaster recovery and business resumption plan developed for the Ohio area office.

Office of Audit Comment: We do not concur with the TE/GE Division's decision to not develop specific disaster and business resumption plans for the LINUS. The risks associated with using the IS Business

Resumption Plan developed for the Ohio area office are increased because the local IS Business Resumption Plan does not specifically identify or refer to the LINUS. Also, the time period to develop the LINUS replacement system may exceed the calendar year 2002 planned implementation date, resulting in additional risks that user fee payment information may be lost.

Conclusion

Even though the TE/GE Division management has initiated actions that may improve the quality, completeness, and reliability of customer user fee account data, additional actions are needed to better manage the data security risks associated with processing user fee payment information on existing systems. Specifically, we determined that additional management emphasis is needed to properly certify and accredit user fee systems and to establish overall responsibility for managing TE/GE Division user fee systems. Also, the TE/GE Division should appoint a functional security coordinator and develop a process for identifying and reporting TE/GE Division automated systems with sensitive information to the Certification Program Office. Additionally, a process should be developed to ensure that Disaster Recovery and Business Resumption Plans are established.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective was to determine whether the Tax Exempt/Government Entities (TE/GE) Division's automated systems used to process user fee payment information provide reasonable assurance that data are properly protected. We:

I. Reviewed the Internal Revenue Service (IRS) data security requirements and performed walk-through evaluations of user fee system processing actions to:

   A. Assess whether the system security controls would minimize unauthorized accesses. Specifically, we:

      1. Reviewed documentation obtained from meetings held with the Director, TE/GE Division Administrative Services unit, and the Letter Information Network User System (LINUS) Systems Administrator.

      2. Reviewed the LINUS System Application Test Plan.

   B. Determine whether an audit trail was used to monitor system accesses. Specifically, we:

      1. Discussed system-monitoring requirements with the TE/GE Division office automation managers and staff and the LINUS Systems Administrator.

      2. Determined if functional security coordinators had been assigned to review system accesses.

   C. Determine whether contingency plans and back-up procedures ensured data would not be lost. Specifically, we:

      1. Reviewed documentation provided by the TE/GE Division field office managers and the LINUS Systems Administrator.

      2. Evaluated the Ohio District Business Resumption Plan and discussed contingency plans for the mid-range computer system maintained at the Martinsburg Computing Center with the Information Systems (IS) organization.

      3. Reviewed the Headquarters Employee Plans/Exempt Organizations Inventory System (HQ EP/EO system) Disaster Recovery and Continuity of Operations planning process.

D. Evaluate the certification/accreditation of user fee payment systems. Specifically, we:

1. Reviewed Office of Management and Budget and IRS guidelines, policies, and requirements relevant to information systems that process sensitive but unclassified taxpayer information.
2. Evaluated plans to re-certify the HQ EP/EO system.
3. Reviewed the Statement of Work for the LINUS.
4. Evaluated the TE/GE Division's efforts for identifying and reporting its automated systems with sensitive but unclassified information to the IS Certification Program Office for addition to the Sensitive Systems Inventory Listing.

II. Interviewed managers and employees responsible for maintaining data security and providing oversight of user fee payment systems to:

A. Evaluate the management structure established by the TE/GE Division to oversee the security of user fee payment data. Specifically, we:

1. Discussed and evaluated oversight responsibilities for the LINUS and the HQ EP/EO system with managers and employees assigned to the TE/GE Division Business Systems unit and the Ohio field office.
2. Identified and analyzed the TE/GE Commissioner's role as the principal accrediting authority for the TE/GE Division's business systems.

B. Evaluate the TE/GE Division's efforts to coordinate data security requirements with the IS organization. Specifically, we:

1. Identified and analyzed the TE/GE Division Business Systems Planning unit's procedures and processes for coordinating and monitoring the services provided by the IS organization.
2. Discussed and evaluated the coordination of data security requirements with the Director, TE/GE Division Business Systems unit.

Appendix II

Major Contributors to This Report

Maurice S. Moody, Associate Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs)
Joseph Edwards, Director
Michael Levi, Audit Manager
Michael Van Nevel, Senior Auditor
Steven Bohrer, Auditor
Marjorie Stephenson, Auditor

Appendix III

Report Distribution List

Commissioner N:C
Deputy Commissioner, Tax Exempt and Government Entities Division T
Chief Counsel CC
Director, Business Systems Planning T:BSP
Director, Employee Plans T:EP
Director, Employee Plans Rulings and Agreements T:EP:RA
Director, Exempt Organizations T:EO
Director, Exempt Organizations Rulings and Agreements T:EO:RA
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Manager EO Determinations T:EO:RA:D
Manager EP Determinations T:EP:RA:D
National Taxpayer Advocate TA
Office of Management Controls N:CFO:F:M
Audit Liaison, Tax Exempt and Government Entities Division T

Appendix IV

Management's Response to the Draft Report

COMMISSIONER
TAX EXEMPT AND
GOVERNMENT ENTITIES
DIVISION

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

RECEIVED
APR 27 2001

APR 27 2001

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Evelyn A. Petschek, Commissioner
Tax Exempt and Government Entities Division

SUBJECT: Response to Draft Audit Report – Additional Management Actions Are Needed to Enhance Data Security When Processing User Fee Payment Information

Thank you for the opportunity to respond to your draft report on user fee payment data.

Your draft report is timely because the Tax Exempt and Government Entities Division (TE/GE) is redesigning our determinations programs computer systems. One part of the redesign project is developing and implementing a new system to control user fee payments submitted by applicants for determination letters. We anticipate the new user fee control system will be ready for use by March 1, 2002. Your report notes limitations in our current systems for controlling user fees, which will help our team as it designs and implements the new system.

As we redesign our user fee control systems, we will retire the Letter Information Network User System (LINUS) in the near future. You recommended many improvements to LINUS. In a few instances, we cannot efficiently accomplish the work required to improve the LINUS system as you recommend before that system is retired. Moreover, to implement some of your recommendations we would have to divert the resources we are currently using to design and implement the new system. You also noted the Headquarters Employee Plans/Exempt Organizations inventory system (HQ EP/EO system). We have no plans to replace this system; however, we asked the Information Systems organization to update its security certification.

We take seriously the responsibility to correctly establish and manage data systems that contain sensitive information. We established within TE/GE a Business Systems Planning office responsible for gathering and documenting requirements for new TE/GE systems development activities and for legacy systems operations and maintenance. We are establishing a formal relationship with Information Systems to certify both our old and new data systems.

Our comments on the specific recommendations in this report are as follows:

IDENTITY OF RECOMMENDATION 1
Emphasize the need to implement processes that will ensure that the TE/GE Division systems are properly certified and accredited.

ASSESSMENT OF CAUSES
The Treasury Inspector General for Tax Administration (TIGTA) found TE/GE management has not established clear guidance regarding the roles and responsibilities for certifying the security of systems used to control user fee payments.

CORRECTIVE ACTIONS
The Commissioner and Deputy Commissioner, TE/GE emphasized to appropriate TE/GE managers the importance of ensuring that TE/GE systems are properly certified and accredited. We established the office of Business Systems Planning to ensure that all TE/GE system development initiatives adhere to the Service's Enterprise Life Cycle (ELC). The ELC, a systems development methodology, establishes security requirements for IRS business systems and safeguards to ensure that we do not deploy new systems without the appropriate security certifications.

IMPLEMENTATION DATE
TE/GE has completed this recommendation.

RESPONSIBLE OFFICIALS
TE/GE has completed this recommendation.

CORRECTIVE ACTIONS MONITORING PLAN
TE/GE has completed this recommendation.

IDENTITY OF RECOMMENDATION 2
Establish a senior-level manager with overall responsibility for managing the security of data for the TE/GE Division's automated systems.

ASSESSEMENT OF CAUSES
TIGTA found TE/GE management has not established clear guidance regarding the roles and responsibilities for certifying the security of systems used to control user fee payments.

CORRECTIVE ACTIONS
The Director, Business Systems Planning and the Division Information Officer will develop a systems inventory matrix to capture and document important information for each of the business systems on which TE/GE relies, including:

- Systems management points of contact,
- Platform and user characteristics,

- Data types, including sensitive but unclassified (SBU) information, and
- Status of security certifications and disaster recovery/business resumption plans.

This matrix will give the Commissioner, TE/GE a basis for monitoring changes and prioritizing follow-up or remedial actions.

IMPLEMENTATION DATE
November 1, 2001

RESPONSIBLE OFFICIALS
Director, Business Systems Planning and Division Information Officer

CORRECTIVE ACTIONS MONITORING PLAN
The Director, Business Systems Planning and the Division Information Officer will give the Commissioner, TE/GE a copy of the matrix.

IDENTITY OF RECOMMENDATION 3
Enhance the service-level agreement (SLA) with the Information Services (IS) organization to ensure that the TE/GE Division's automated systems are timely certified that data will be properly safeguarded.

CORRECTIVE ACTIONS
We do not yet have a formal SLA between TE/GE and the IS organization; however, we are planning one. We do require all our system development initiatives to adhere to the Service's Enterprise Life Cycle. This will ensure that we do not deploy new systems without appropriate security certifications and data safeguards. Our commitment to adhere to the ELC thus satisfies the intent and purpose of this recommendation.

IMPLEMENTATION DATE
TE/GE has completed this recommendation.

RESPONSIBLE OFFICIALS
TE/GE has completed this recommendation.

CORRECTIVE ACTIONS MONITORING PLAN
TE/GE has completed this recommendation.

IDENTITY OF RECOMMENDATION 4
Ensure that automated systems require unique and secure password information and the ability to monitor employee access.

ASSESSMENT OF CAUSES
This recommendation concerns the integrity of the audit trail for user access to LINUS. TIGTA found that the LINUS design did not enable the system to generate or accept secure user identification passwords. Further, employees use readily available

employee identification numbers as passwords to access LINUS, thereby compromising the integrity of the audit trail.

However, LINUS is not an unprotected system. Knowledge of another employee's employee identification number is not sufficient to gain access to the specific PC. LINUS is protected by three levels of security. A user must:

1. Gain physical access to the secured area where the PCs are located through which one can gain access to LINUS.
2. Know which PC has a specific LINUS client on it; a specific LINUS client is accessible from only one PC.
3. Know the password to the specific PC to gain access.

CORRECTIVE ACTIONS
TE/GE will require that system development initiatives adhere to the ELC to ensure that we complete security certifications appropriate for the data contained in the systems before we deploy the systems.

We will retire LINUS in the near future. Therefore, we have asked IS Security to help us assess the vulnerabilities within LINUS and identify interim solutions necessary and cost effective for a system with a limited system life. TE/GE will ask IS to act based on the needs identified.

IMPLEMENTATION DATE:
October 1, 2001.

RESPONSIBLE OFFICIALS
Director, Business Systems Planning; Division Information Officer

CORRECTIVE ACTIONS MONITORING PLAN
The Director BSP and the DIO will present recommendations for modifications to LINUS to the Deputy Commissioner, TE/GE.

IDENTITY OF RECOMMENDATION 5
Emphasize the need to generate audit trail reports for review of system access on all systems used to process user fee payment information.

ASSESSMENT OF CAUSES
The HQ EP/EO system is run on hardware that does not have the capacity to generate audit trail reports. Although LINUS is capable of generating an audit trail, TIGTA found that no one has been assigned responsibility to produce and review audit trail reports.

CORRECTIVE ACTIONS
TE/GE plans to migrate the HQ EP/EO system from its current hardware to a new SUN platform. When this takes place, the hardware will have sufficient capacity to generate audit trail reports. At that time, the Director, EO Rulings and Agreements will require the HQ EP/EO data base administrator to produce audit trail reports for review by the HQ EP/EO functional security coordinator. The Director, Exempt Organizations (EO) Rulings and Agreements will require the LINUS data base administrator to produce audit trail reports for review by the LINUS functional security coordinator.

IMPLEMENTATION DATE
October 1, 2001

RESPONSIBLE OFFICIALS
Director, EO Rulings and Agreements

CORRECTIVE ACTIONS MONITORING PLAN
The data base administrator of each system will generate and provide audit trail reports to the functional security coordinator of each system.

IDENTITY OF RECOMMENDATION 6
Appoint a functional security coordinator for LINUS who will conduct periodic functional security reviews using system-generated audit trail information.

ASSESSMENT OF CAUSES
Although LINUS can generate an audit trail, TIGTA found that we have not given anyone responsibility to produce and review audit trail reports.

CORRECTIVE ACTIONS
The Director, EO Rulings and Agreements will appoint a functional security coordinator for LINUS.

IMPLEMENTATION DATE
October 1, 2001

CORRECTIVE ACTIONS MONITORING PLAN
The Director, EO Rulings and Agreements will report to the Director, EO that he ahs appointed LINUS functional security coordinator.

IDENTITY OF RECOMMENDATION 7
Develop a process for identifying and reporting the TE/GE Division's automated systems with sensitive information to the Certification Program Office

ASSESSMENT OF CAUSES
LINUS is not listed as a system with sensitive information on the Sensitive Systems Inventory Listing. Additionally, TIGTA found that we have not given any TE/GE

manager responsibility for reporting systems with sensitive but unclassified information to the Certification Program Office.

CORRECTIVE ACTIONS
The Director, Business Systems Planning and the Division Information Officer will develop a systems inventory matrix to capture and document important information for each of the business systems TE/GE relies on. The matrix will identify any system with sensitive information not reported to the Certification Program Office. If we identify such systems, we will report them. When we arrange for the development of future business systems, we will require the developers to comply with the Enterprise Life Cycle process, thereby ensuring that we complete appropriate security certifications before deploying the systems. This process includes registering appropriate systems with the Certification Program Office.

IMPLEMENTATION DATE
November 1, 2001

RESPONSIBLE OFFICIALS
Director, Business Systems Planning and Division Information Officer

CORRECTIVE ACTIONS MONITORING PLAN
The Director, Business Systems Planning and the Division Information Officer will give the Commissioner, TE/GE a copy of the matrix and identify any system not registered with the Certification Program Office.

IDENTITY OF RECOMMENDATION 8
Develop a process to ensure we develop the Disaster Recovery and Business Resumption Plans for LINUS.

ASSESSMENT OF CAUSES.
TIGTA found that the local business resumption plan for the Ohio district did not specifically identify or refer to LINUS.

CORRECTIVE ACTIONS
TE/GE is redesigning the Employee Plans and Exempt Organizations Determination System (EDS). We will replace LINUS with a new system for controlling user fee payments. We are developing the redesigned system according to the Enterprise Life Cycle. This process requires us, among other things, to develop a disaster recovery and business resumption plan for the new system. Thus, the successor to LINUS will be covered by such a plan. In the meantime, we are using the Ohio district disaster and business resumption plan to protect LINUS, even though it does not specifically refer to LINUS.

Therefore, we do not accept the recommendation to develop a Disaster Recovery and Business Resumption Plan for LINUS. We will retire LINUS early in calendar year 2002

and believe that developing a separate Disaster Recovery and Business Resumption Plan for LINUS is not cost effective.

IMPLEMENTATION DATE
TE/GE declines to accept this recommendation.

RESPONSIBLE OFFICIAL
TE/GE declines to accept this recommendation.

CORRECTIVE ACTION MONITORING PLAN
TE/GE declines to accept this recommendation.

If you have any questions or need additional information, please call me at (202) 283-2500, or a member of your staff may contact Mike Daly at 283-8885.